ID: 800684
Cookbook: browseurl.jbs
Time: 18:06:28
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report http://www.familyproof.com 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 9
World Map of Contacted IPs 15
Public IPs 15
Private 17
General Information 18
Warnings 18
Simulations 18
Behavior and APIs 18
Joe Sandbox View / Context 19
IPs 19
Domains 19
ASNs 19
JA3 Fingerprints 19
Dropped Files 19
Created / dropped Files 19
Static File Info 19
Network Behavior 19
Statistics 19
Behavior 19
System Behavior 20
Analysis Process: chrome.exePID: 5932, Parent PID: 1836 20
General 20
File Activities 20
Registry Activities 20
Analysis Process: chrome.exePID: 3460, Parent PID: 5932 20
General 20
File Activities 20
Analysis Process: chrome.exePID: 4516, Parent PID: 1836 21
General 21
Registry Activities 21
Disassembly 21

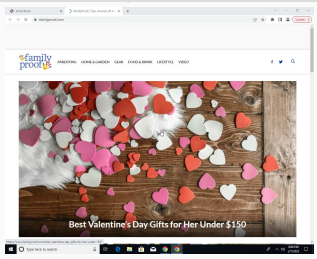
Windows Analysis Report

http://www.familyproof.com

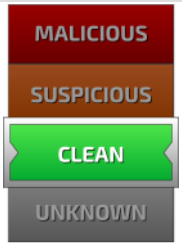
Overview

General Information

Sample URL:	http://www.familyproof.com
Analysis ID:	800684
Infos:	



Detection

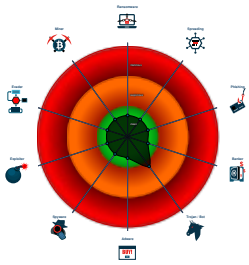


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Connects to several IPs in different …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5932 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 3460 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1884 --field-trial-handle=1648,i,15664817480715420111,2584482007518194518,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4516 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://www.familyproof.com MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

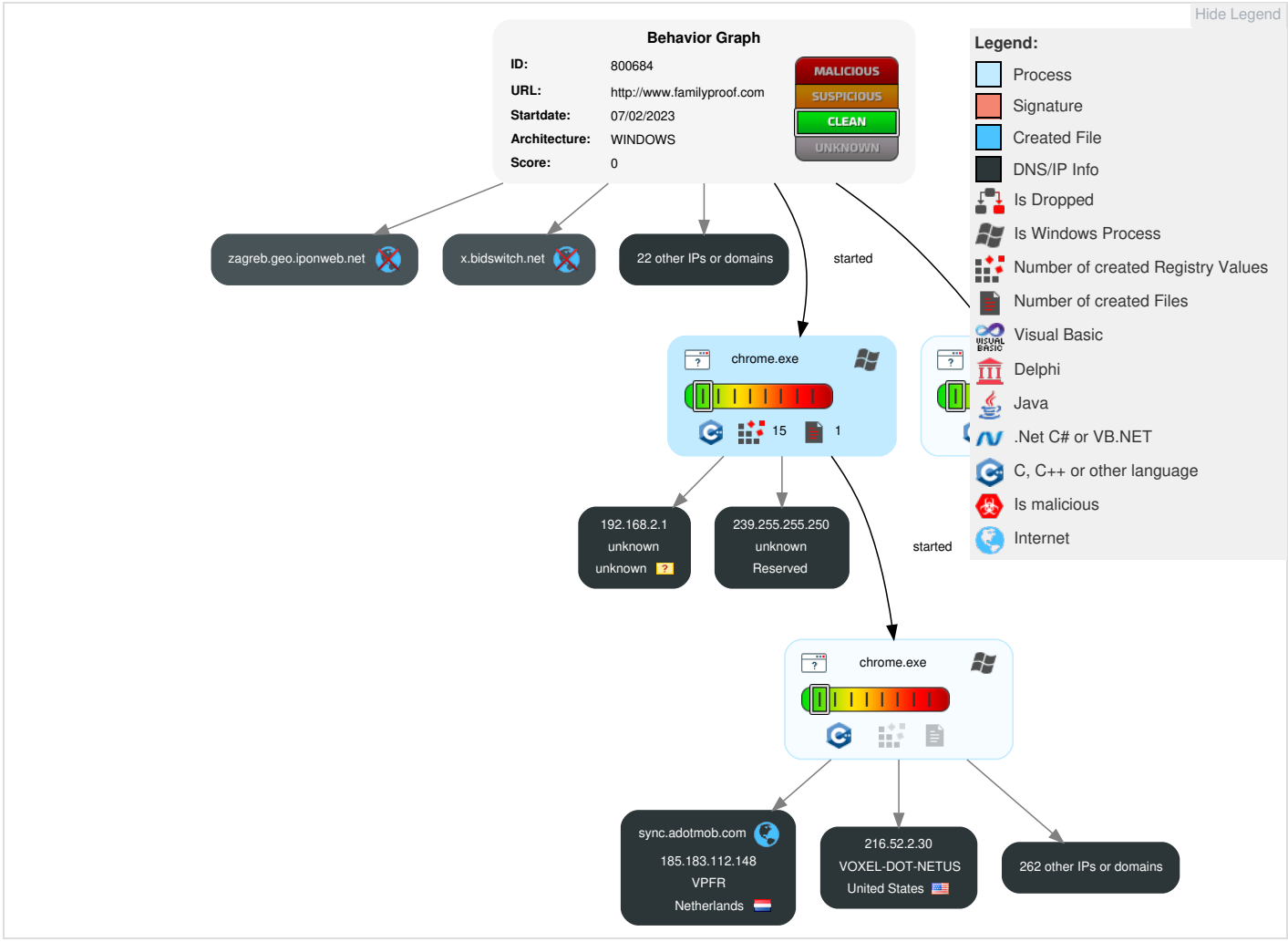
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

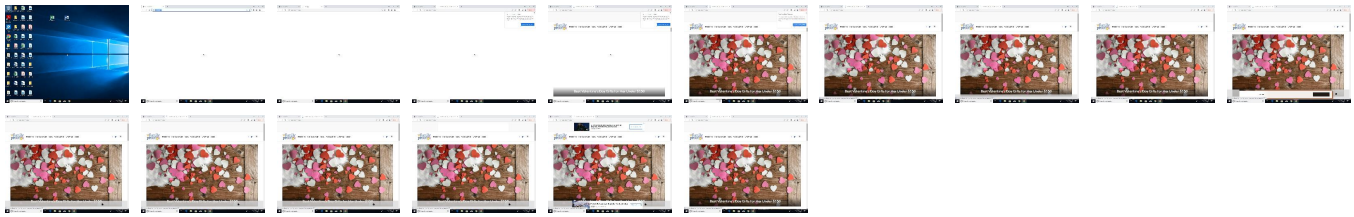
Behavior Graph

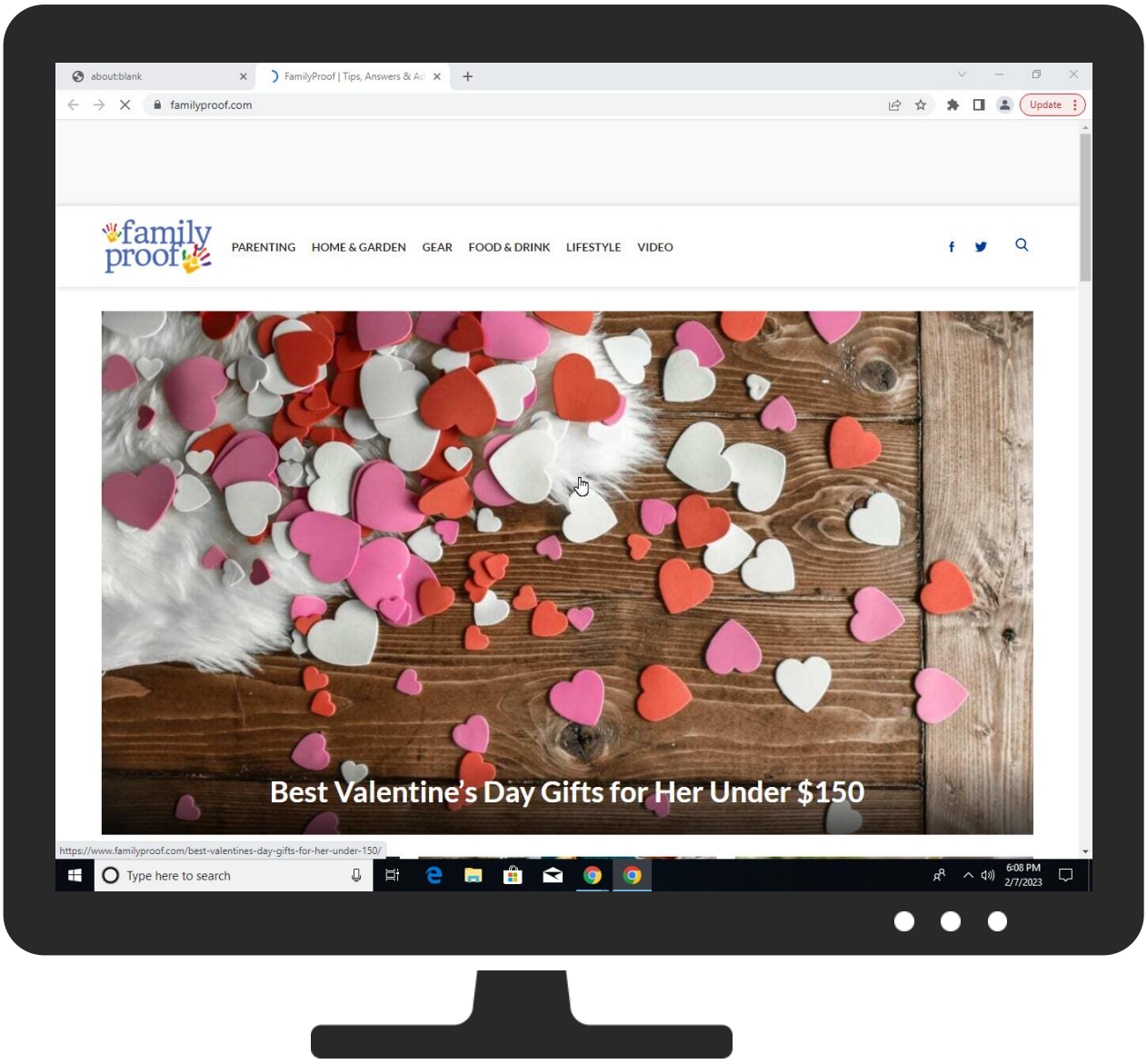


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://www.familyproof.com	1%	Virustotal		Browse
http://www.familyproof.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.familyproof.com/wp-content/mu-plugins/tpd-featured-posts/dist/blocks.style.build.css?ver=1.89	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://id5-sync.com/g/v2/1120.json	0%	Avira URL Cloud	safe	
http://https://www.familyproof.com/wp-content/uploads/2023/01/element5-digital-WAiyQLGEEc-unsplash-1180x788.jpg	0%	Avira URL Cloud	safe	
http://https://match.prod.bidr.io/cookie-sync/mo?	0%	Avira URL Cloud	safe	
http://https://www.familyproof.com/wp-content/uploads/2023/01/photo-1519708227418-c8fd9a32b7a2-428x285.webp	0%	Avira URL Cloud	safe	
http://https://x.bidswitch.net/sync?ssp=triplelift&user_id=42594309756452850305l8&gdpr=0&gdpr_consent=	0%	Avira URL Cloud	safe	
http://https://pixel-eu.onaudience.com/?partner=270&smartmap=1&gdpr=0&gdpr_consent=&redirect=image2.pubmatic.com%2FAdServer%2FPug%3Fvcode%3Dbz0yJnR5cGU9MSZjb2RlPTI4ODQmdGw9MTI5NjAw%26piggybackCookie%3D%25_rid%26gdpr%3D0%26gdpr_consent%3D%25_gdpr_consent	0%	Avira URL Cloud	safe	
http://https://a.audrte.com/p	0%	Avira URL Cloud	safe	
http://https://prebid.a-mo.net/cchain/0?gdpr=&us_privacy=&cb=https%3A%2F%2Fprebid.tpdads.com%2Fsetuid%3Fbidder%3Damx%26gdpr%3D%26gdpr_consent%3D%26f%3Di%26uid%3D	0%	Avira URL Cloud	safe	
http://https://get.geojs.io/v1/ip/country.json	0%	Avira URL Cloud	safe	
http://https://www.familyproof.com/wp-content/uploads/2023/01/brooke-lark-jUPOXXRNdcA-unsplash-788x444.jpg	0%	Avira URL Cloud	safe	
http://https://prebid.tpdads.com/setuid?bidder=medianet&gdpr=&gdpr_consent=&f=i&uid=0000EEA	0%	Avira URL Cloud	safe	
http://https://www.familyproof.com/wp-includes/js/jquery/jquery.min.js?ver=3.6.1	0%	Avira URL Cloud	safe	
http://https://www.familyproof.com/	0%	Avira URL Cloud	safe	
http://https://www.familyproof.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://www.familyproof.com/wp-content/uploads/2023/01/child_boy_game_package_box_kid_gift_moving_to-917512-788x444.jpg	0%	Avira URL Cloud	safe	
http://https://u.4dex.io/setuid?bidder=indexexchange&uid=Y-KFdBYMDP6MQHUBZ5vSBQAABIUAAAAB	0%	Avira URL Cloud	safe	
http://https://prebid.tpdads.com/openrtb2/auction	0%	Avira URL Cloud	safe	
http://https://x.bidswitch.net/check_uuid/https%3A%2F%2Faax-eu.amazon-adsystem.com%2Fs%2Fecm3%3Fex%3Dmediagrid.com%26id%3D%24%7BBSW_UUID%7D	0%	Avira URL Cloud	safe	
http://https://cdn.p-n.io/pushly-sdk.min.js?domain_key=tuYtwQ25XFtJZbspIunR6b5BjhiurM3ckeEC&ver=6.1.1	0%	Avira URL Cloud	safe	
http://https://rtb.mfadsrvr.com/ul_cb/sync?ssp=yieldmo	0%	Avira URL Cloud	safe	
http://https://www.familyproof.com/wp-content/mu-plugins/tpd-featured-posts/src/slick-carousel/slick.min.js?ver=1.8.1	0%	Avira URL Cloud	safe	
http://https://k.p-n.io/event-stream	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
um.simpli.fi	34.91.62.186	true	false		high
lga-bh-bgp.contextweb.com	198.148.27.140	true	false		high
global.px.quantserve.com	91.228.74.206	true	false		high
id5-sync.com	162.19.138.120	true	false		unknown
api.parsely.com	54.87.63.104	true	false		high
pixel-a.sitescout.com	98.98.134.241	true	false		high
envoy1.envoy-csync1.core-b8mf.ov1o.com	35.214.223.115	true	false		unknown
p1.parsely.com	63.34.81.234	true	false		high
prebid.a-mo.net	147.75.85.234	true	false		unknown
ads-yieldmo-com-eu-west-1-544050270.eu-west-1.elb.amazonaws.com	52.19.249.135	true	false		high
mwzeom.zeotap.com	104.22.25.87	true	false		high
www.google.com	142.250.184.100	true	false		high
match.adsrvr.org	52.223.40.198	true	false		high
match.prod.bidr.io	52.213.61.172	true	false		unknown
rtb-csync-itx5.smartadserver.com	185.86.138.145	true	false		high
pagead-googlehosted.l.google.com	142.251.209.1	true	false		high
chidc2.outbrain.org	50.31.142.191	true	false		unknown
creativecdn.com	185.184.8.90	true	false		high
pugm-lhrc.pubmnet.com	185.64.190.78	true	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d1qug1xf2dk5z6.cloudfront.net	13.224.103.60	true	false		high
uip.semasio.net	77.243.60.138	true	false		high
pixel.onaudience.com	141.94.170.64	true	false		unknown
dgcbxsxpz6nta.cloudfront.net	13.224.98.168	true	false		high
d1ykf07e75w7ss.cloudfront.net	13.224.100.141	true	false		high
optimon.appspot.com	142.251.143.148	true	false		unknown
googleads.g.doubleclick.net	142.250.180.130	true	false		high
ads.travelaudience.com	35.190.0.66	true	false		high
www.familyproof.com	104.26.13.214	true	false		unknown
clients.l.google.com	142.250.180.174	true	false		high
in-appadvertising.com	169.63.109.126	true	false		unknown
www.googletagservices.com	142.251.209.34	true	false		high
id.crwdcntrl.net	79.125.68.7	true	false		high
hbx.media.net	2.18.160.23	true	false		high
iad-2-sync.go.sonobi.com	69.166.1.10	true	false		high
cc.adingo.jp	54.199.165.234	true	false		unknown
adservice.google.com	142.251.209.34	true	false		high
ssbsync-itx5.smartadserver.com	185.86.138.151	true	false		high
oeu.vap.lijit.com	216.52.2.48	true	false		high
pixel-eu.onaudience.com	141.94.171.214	true	false		unknown
core.iprom.net	195.5.165.20	true	false		unknown
contextual.media.net	23.211.6.95	true	false		high
b1-eudc1.zemanta.com	213.227.153.220	true	false		high
api.rlcdn.com	34.120.133.55	true	false		high
dyv1bugovvq1g.cloudfront.net	13.224.98.18	true	false		high
spug-lhrc.pubmnet.com	185.64.190.81	true	false		unknown
sync.richaudience.com	162.55.236.225	true	false		high
outbrain.map.fastly.net	146.75.122.132	true	false		unknown
sync.srv.stackadapt.com	52.0.142.7	true	false		high
d5p.de17a.com	213.155.156.165	true	false		high
sync.adotmob.com	185.183.112.148	true	false		high
pagead46.l.doubleclick.net	142.250.184.98	true	false		high
accounts.google.com	216.58.209.45	true	false		high
ad.doubleclick.net	142.250.180.166	true	false		high
s.amazon-adsystem.com	52.46.128.147	true	false		high
cdn.confiant-integrations.net	104.18.17.107	true	false		unknown
aax-eu.amazon-adsystem.com	52.94.223.37	true	false		high
fr-xn.lb.indexww.com	185.80.39.216	true	false		unknown
ipac.ctnsnet.com	35.186.193.173	true	false		high
idsync.frontend.weborama.fr	34.111.131.239	true	false		high
elb-aws-fr-zagreb-1702672115.eu-central-1.elb.amazonaws.com	18.193.49.80	true	false		high
match.adsby.bidtheatre.com	159.65.194.197	true	false		unknown
gum.am5.vip.prod.criteo.com	178.250.2.146	true	false		high
d2dwiwtjj7ipd3.cloudfront.net	13.224.103.30	true	false		high
ib.anycast.adnxs.com	185.89.211.84	true	false		high
prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	3.126.56.137	true	false		unknown
matching.truffle.bid	157.90.40.26	true	false		unknown
queue.amazonaws.com	3.236.169.43	true	false		high
btlr-ecs-eu-central-1.sharethrough.com	3.125.220.90	true	false		high
protected-by.clarium.io	52.209.237.217	true	false		unknown
eu-u.openx.net	35.244.159.8	true	false		high
ws.rqtrk.eu	141.95.97.230	true	false		unknown
spl.zeotap.com	104.22.24.87	true	false		high
eu-eb2.3lift.com	13.248.245.213	true	false		high
obs.cheqzone.com	50.16.211.97	true	false		unknown
1x1.a-mo.net	3.215.74.86	true	false		unknown
k.p-n.io	18.159.168.223	true	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com	35.156.20.158	true	false		high
bidder-eu-central-1.prod.justpremium.com	18.194.224.59	true	false		high
script.4dex.io	104.26.9.169	true	false		unknown
widget.am5.vip.prod.criteo.com	178.250.2.151	true	false		high
pug22000nfc.pubmnet.com	185.64.189.110	true	false		unknown
sync.crwdcntrl.net	54.194.53.119	true	false		high
tagr-gcp-odr-euw4.mookie1.com	34.98.67.61	true	false		high
cm.g.doubleclick.net	142.250.180.162	true	false		high
sync.1rx.io	213.19.147.45	true	false		high
ds-pr-bh.ybp.gysm.yahoodns.net	52.30.151.89	true	false		unknown
prod.us-east-1.cxm-bcn.publisher-services.amazon.dev	107.21.165.221	true	false		unknown
cdn-content.ampproject.org	142.250.180.129	true	false		high
mp.4dex.io	104.18.2.114	true	false		unknown
prebidtest.zemanta.com	104.22.7.45	true	false		high
zemanta.map.fastly.net	151.101.2.132	true	false		unknown
spug-amsfpairbc.pubmnet.com	198.47.127.20	true	false		unknown
ads.playground.xyz	34.102.253.54	true	false		unknown
us-u.openx.net	35.244.159.8	true	false		high
securepubads46.g.doubleclick.net	142.250.180.130	true	false		high
cm-supply-web.gammaplatform.com	52.220.229.2	true	false		high
elb-aws-fr-dorpat-283474803.eu-central-1.elb.amazonaws.com	3.122.125.162	true	false		high
dsp.adfarm1.adition.com	85.114.159.93	true	false		high
d1jvc9b8z3vcjs.cloudfront.net	13.224.89.76	true	false		high
cs.media.net	2.18.160.23	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://nym1-ib.adnxs.com/ab?an_audit=0&referrer=https%3A%2F%2Fwww.familyproof.com%2F&e=wqT_3QK5Dei5BgAAAwDWAAUBCJyLip8GEJvV9-K9xZq8MRjK5ei6xcrY8FAqNgkB0OM0hRDmPxE0I3Kw7ePePxkAAAECUNA_ISnv42iOrN8_KR09fm_Tn-Y_MQEZuAAA0D8w75LJBji6GUC5XEgCUL32usYBWLCPYGAAaPrFRHiOtQWAAQGKAQNVU0SSBQbgmAHYBaABWqgBAbABALgBAsABBcgBAtABCdgBAOABAPABAIoCaXVmKCdhJywgNTg5NzY5MSwgMCk7ARQsaScsIDc0ODMxNjMsERQsZycsIDE4NjMxMzUyFRUwcycsIDI3Njk5NjMzMBUWLHInLCA0MTYyMDE1MwIB8LaSAtkEIWxuTGc5d2lrXzhVWkVMMzJ1c1ICR0FBZ3NJOWdNQUE0QUVBQVNMbGNVTy1TeVFaWUFHQ3FBMmdBY0FCNEFJQUJBSWdCQUpBQkFaZ0JBYUFCQWFnQkFiQUJBTGtCTUloVnBJMzI1RF9CQVRWRm8wYkpuLVlfeVFFQUFBQUFBQUR3UDlrQjlCV2tHWXVtN1RfZ0FadmV5QVAxQVdpMHB6LVlBZ0NnQWdHMUFnQUFBQUM5QWcBOfBMREFBZ0RJQWdEUUFnRFlBZ0RnQWdEb0FnRDRBZ0NBQXdHWUF3R2lBdzRJNXBYS0l4QUJHQUl0QUFEQVA2SURGd2ptb1lnbEVBSVlBUzABUfBVQU1nZGtaV1poZFd4MG9nTU9DT2FWeWlNUUN4Z0NMUUFBd0QtNkF3bE9XVTB5T2pRMk5URGdBN1V3Z0FTVDA1QUtpQVNVMDVBS2tBUUJtQVFCd1FRQUEFWhRBQUFNa0UBBwkBGERZQkFEeElJDQUBQGlBV3FKSmdGNnNHS2hBR3BCETsUUEFfc1FVBSQFAQhNRUYFCBhBQUEtRF9KBSgcS0JtOC1zXzAuKAAETmsVKMA4RF9nQmEyb0JQQUZ1Slh4Q1BnRjJfdm5Bb0lHQTBOSVJvZ0dCSkFHQVpnR0FLRUdBAV04QUFBOEQtb0JnU3lCaVFKARANAQBSDQgBAQBaAQUNAQBoDQhIQUFBQzRCZ28umgKZASFSaFd4Nz5dAihMQ1BZQ0FBS0FBeAEvAQGIOEQ4NkNVNVpUVEk2TkRZMU1FQzFNRW4wRmFRWmk2YnRQMUUBJwkBBEZrCQgBAQBHPVgARx0YAEgdGAxIZ0FpLnEC8EZ3Li7YAshD4ALL6CTqAhxodHRwczovL3d3dy5mYW1pbHlwcm9vZi5jb20v8gIRCgZBRFZfSUQSBzU4OTc2OTHyAhIKBkNQRwEUAAhxfAEVCAVDUAEUAAl1ezjyAg0KCEFEVl9GUkVREgEJEBxSRU1fVVNFUgUQAAwJIBhDT0RFEgDyAQ8BWREPEAsKB0NQFQ4QEAoFSU8BYQAHjQUA8gEhBEIPFSE4EwoPQ1VTVE9NX01PREVMASsUAPICGgoWMhYAHExFQUZfTkFNBXEIHgoaNh0ACEFTVAE-EEIGSUVEAT4cFQoIU1BMSVQBTRnZ8NCAAwCIAwGQAwCYAxSgAwGqAwDAA6wCyAMA2AOzzZMB4AMA6AMA-AMDgAQAkgQJL29wZW5ydGlymAQAogQLODQuMTcuNTIuMTOoBACyBAwIABAAGAAgADAAOAC4BADABJ6n9iHIBADSBA8xMTgzMyNOWU0yOjQ2NTDaBAIIAeAEAPAEvfa6xgGIBQGYBQCgBf_____wGqBSQzNmZlZTI5OC1hYmM2LTRhYzAtYWRlMi1jYTQ3ZDNmMjQwN2bABQDJBQAAAAAAPA_0gUJCanQeAAA2AUB4AUB8AWangT6BQQIABAAkAYAmAYAuAYAwQYJJSzwP9AG-Y8B2gYWChAJEhkBAchk4AYB8gYCCACABwGIBwCgBwHIB461BdIHDQkRKAEmCNoHBgFecBgA4AcA6gcCCADwB8aDDYoIAhAAlQgAAIA_mAgB&s=a5fb6f7619529c6a4beefe76979d137fdc1f88fd&pp=0.482662	false		high
http://https://ib.adnxs.com/getuid?https%3A%2F%2Fce.lijit.com%2Fmerge%3Fpid%3D92%263pid%3D%24UID&gdpr=0&gdpr_consent=	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://securepubads.g.doubleclick.net/pagead/adview?ai=CTxzjb4XiY-DnL8il9u8Pq42NcOCI-61uzJqwyLUQpK_1yZI1EAEgjJuEImC7BqABgaGkuSjIAQLgAgCoAwHIAwiqBPgBT9A6HXUKEZvKbZUZoc30NtTBeXsPrwIOV_7UW8ianS3m4D5MrZFWUmQpV97hEY-eD3EjBITOzwXSy0ZI-GtKkM6JCCppm2wIVbR4RJTaCTieMz1ephaAa13Q2URJgOFTKgpz40TlnBLeNJHqLs695dnB3u_VkNC7oTOukE4eQwy7_DBEgXF6VVZJbwEH8PTVYM9s5AT2t3DcmmZhvGK-xujvV9JfPnRsjTLieaVDzhQZOUlQqLTZ8CsBryJngH0l4zbl0hz1iB7zZXng5f7sK59L2BmJLXKoDv_Brw49CPdR8rpox7Kh1LRKSjBv_afC60NRObcvb7fABJfZx-KiBOAEAZIFBAgEGAGSBQQIBRgEkgUECAUYGJIFBQgFGKgBoAYCgAeB2fSYA6gHjs4bqAeT2BuoB-6WsQKoB_6esQKoB6SjsQKoB9XJG6gHpr4b2AcB8gcEENm8l9IIEQiA4YAQEAEYHTICqgI6AoBAgAoDyAsB2BMM0BUBmBYBgBcBshceChwIABIUcHViLTIzMjIxNTc4Njk2MDk0NDkY_MgX&sigh=DRHWqRWI__0&uach_m=[UACH]&cid=CAQSPADUE5ym7biyk9YBYbWTvIYrUtlPoOkjpGUK1fAwECLdm9-LOLFUg6yuoTofgcta3fCXzYl8zHNQx48gKBgB	false		high
http://https://securepubads.g.doubleclick.net/gpt/pubads_impl_2023020201.js	false		high
http://https://aax-eu.amazon-adsystem.com/x/px/JKlc_E30RxHrDvVAJVrpXxEAAAGGLNk5NwMAAAJYAQBhcHNfdHhuX2JpZDEgICBOL0EgICAgICAgICCF6U5X/v/%7B%22v%22:%7B%22p%22:0,%22t%22:0,%22def%22:%22amzn%22%7D,%22vs%22:%22visible%22,%22ah%22:90,%22aw%22:728,%22ttv%22:2.76,%22ts%22:1675822100739,%22bn%22:false,%22pixelId%22:%22gsn4veez8kp%22,%22ver%22:%22r-1.30%22%7D?cb=498238	false		high
http://https://simage2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTM0MDEmdGw9NDMyMDA=&piggybackCookie=5828047507176436426	false		high
http://https://d5p.de17a.com/getuid/pubmatic;c?https://image2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTI3NDUmdGw9MTI5NjAw&gdpr=0&gdpr_consent=&piggybackCookie=$UID	false		high
http://https://d15kdpgjg3unno.cloudfront.net/oPS.js?cid=68	false		high
http://https://cdn.ampproject.org/rtv/012301242213000/v0/amp-form-0.1.mjs	false		high
http://https://g2.gumgum.com/hbid/imp?lt=1675822065251&to=480&aun=dsk-banner-ad-b&t=0ed7c58f&pi=3&maxw=970&maxh=90&si=945925&bf=970x90%2C728x90%2C468x60%2C320x50%2C300x100%2C1x1&schain=1.0%2C1!publisherdesk.com%2C100337%2C1%2C%2C%2C&vw=1280&vh=913&sw=1280&sh=1024&pu=https%3A%2F%2Fwww.familyproof.com%2F&ce=true&dpr=1&jcsi=%7B%22t%22%3A0%2C%22rq%22%3A8%2C%22pbv%22%3A%227.32.0%22%7D&ogu=https%3A%2F%2Fwww.familyproof.com%2F&ns=10138	false		high
http://https://aax-eu.amazon-adsystem.com/s/ecm3?ex=smart.com&id=5613407791116526711&gdpr=0&gdpr_consent=	false		high
http://https://cm.g.doubleclick.net/pixel?google_nid=openx&google_cm&google_sc	false		high
http://https://www.familyproof.com/wp-content/mu-plugins/tpd-featured-posts/dist/blocks.style.build.css?ver=1.89	false	• Avira URL Cloud: safe	unknown
http://https://s.amazon-adsystem.com/ecm3?ex=rubiconprojectHMT&id=NXSdU0W2QUu-Er1Zvpq2ZA	false		high
http://https://d5p.de17a.com/getuid/pubmatic?https://image2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTI3NDUmdGw9MTI5NjAw&gdpr=0&gdpr_consent=&piggybackCookie=$UID	false		high
http://https://www.familyproof.com/wp-content/uploads/2023/01/photo-1519708227418-c8fd9a32b7a2-428x285.webp	false	• Avira URL Cloud: safe	unknown
http://https://ad.doubleclick.net/ddm/trackimp/N1427610.1943701GDN/B25836967.304034198;dc_pre=CM-jw4bzg_0CFTWC_QcdGd4GHA;dc_trk_aid=513334743;dc_trk_cid=151320179;ord=621618055;dc_lat=;dc_rdid=;tag_for_child_directed_treatment=;tfua=;gdpr=;gdpr_consent=;ltd=?	false		high
http://https://g2.gumgum.com/hbid/imp?lt=1675822065266&to=480&aun=dsk-box-ad-b&t=0ed7c58f&pi=3&maxw=300&maxh=600&si=945933&bf=300x600%2C300x250%2C160x600%2C120x600&schain=1.0%2C1!publisherdesk.com%2C100337%2C1%2C%2C%2C&vw=1280&vh=913&sw=1280&sh=1024&pu=https%3A%2F%2Fwww.familyproof.com%2F&ce=true&dpr=1&jcsi=%7B%22t%22%3A0%2C%22rq%22%3A8%2C%22pbv%22%3A%227.32.0%22%7D&ogu=https%3A%2F%2Fwww.familyproof.com%2F&ns=10138	false		high
http://https://aax-eu.amazon-adsystem.com/x/px/JKlc_E30RxHrDvVAJVrpXxEAAAGGLNk5NwMAAAJYAQBhcHNfdHhuX2JpZDEgICBOL0EgICAgICAgICCF6U5X/atf/%7B%22atf%22:true,%22f%22:1,%22vs%22:%22visible%22,%22ah%22:90,%22aw%22:728,%22ts%22:1675822100740,%22bn%22:false,%22pixelId%22:%22gsn4veez8kp%22,%22ver%22:%22r-1.30%22%7D?cb=1096667	false		high
http://https://www.familyproof.com/wp-content/uploads/2023/01/element5-digital-WAiyQLGEEc-unsplash-1180x788.jpg	false	• Avira URL Cloud: safe	unknown
http://https://match.prod.bidr.io/cookie-sync/mo?	false	• Avira URL Cloud: safe	unknown
http://https://g2.gumgum.com/hbid/imp?lt=1675822124134&to=480&aun=dsk-banner-ad-b&criteoId=qXfxHl9VSiUyRmx5anUlMkZLUW8lMkZEU0c5TW9tV3k0cnE5czIwcE1ocDFqMkMlMkZBaEIzemRRWm51QjZ1JTJGNmp0MnFyUUNUQXFlaSUyRmtMJTJCeXRBalFkTlIGTWxTWTI3clRRJTNEJTNE&id5id=0&pubcid=b2844ada-ab41-4456-ac98-1839b08794a2&pv=4f0e54de-cc91-49b1-80b0-ada2cac20de2&fp=0.25&fpc=USD&t=0ed7c58f&pi=3&maxw=970&maxh=90&si=945926&bf=970x90%2C728x90%2C468x60%2C320x50%2C300x100%2C1x1&schain=1.0%2C1!publisherdesk.com%2C100337%2C1%2C%2C%2C&vw=1280&vh=913&sw=1280&sh=1024&pu=https%3A%2F%2Fwww.familyproof.com%2F&ce=true&dpr=1&jcsi=%7B%22t%22%3A0%2C%22rq%22%3A8%2C%22pbv%22%3A%227.32.0%22%7D&ogu=https%3A%2F%2Fwww.familyproof.com%2F&ns=5734	false		high
http://https://ap.lijit.com/beacon/amazon?url=https://aax-eu.amazon-adsystem.com%2Fs/ecm3?id=$UID&ex=sovrn.com	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://id5-sync.com/g/v2/1120.json	false	• Avira URL Cloud: safe	unknown
http://https://adservice.google.com/adsid/integrator.js?domain=www.familyproof.com	false		high
http://https://x.bidswitch.net/sync?ssp=triplelift&user_id=42594309756452850305 18&gdpr=0&gdpr_consent=	false	• Avira URL Cloud: safe	unknown
http://https://securepubads.g.doubleclick.net/gampad/ads?pvsid=4287636170759586&correlator=3848810272311789&eid=31072031%2C31072039&output=ldjh&gdfp_req=1&vrg=2023020201&ptt=17&impl=fif&iu_parts=134702932%2C0337-familyproof.com-oop%2C0337-oop-ad-a&enc_prev_ius=%2F0%2F1%2F2&prev_iu_szs=1x1&ifi=6&adks=3108343253&sfv=1-0-40&prev_scp=position%3Doop-ad-a%26refreshcount%3D1%26refresh%3Dfalse&eri=1&cust_params=domain%3Dfamilyproof.com%26Page-Type%3Dhome%26URL%3Dhttps%253A%252F%252Fwww.familyproof.com%252F%26session_id%3DU1dwherEdbke76Q%26path%3D%252F%26url%3D%252F%26kw%3DFamilyProof%252C%257C%252CTips%252C%252CAnswers%252C%2526%252CAdvice&sc=1&cookie=ID%3De865e957478f33a0-2220b777e9da0015%3AT%3D1675789665%3ART%3D1675789665%3AS%3DALNI_MZ7qAbgfbuZ3Skh2x9KZ9GpQbihDA&gpic=UID%3D00000bb1552dc58c%3AT%3D1675789665%3ART%3D1675789665%3AS%3DALNI_MYUho0SSsKXSuGrPy5e7JP866nApA&abxe=1&dt=1675822078692&lmt=1675822078&dlt=1675822060272&idt=4785&adxs=0&adys=0&biw=1263&bih=913&scr_x=0&scr_y=0&btvi=0&ucis=5&oid=2&u_his=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_sd=1&u_tz=-480&dmc=8&bc=31&uach=WyJXaW5kb3dzIiwiNi4wLjAiLCJ4ODYiLCIiLCIxMDQuMC41MTEyLjgxIixbXSxmYWxzZSxudWxsLCI2NCIsW1siQ2hyb21pdW0iLCIxMDQuMC41MTEyLjgxIl0sWyIgTm90IEE7QnJhbmQiLCI5OS4wLjAuMCJdLFsiR29vZ2xlIENocm9tZSIsIjEwNC4wLjUxMTIuODEiXV0sZmFsc2Vd&nvt=1&url=https%3A%2F%2Fwww.familyproof.com%2F&frm=20&vis=1&psz=1263x4252&msz=0x0&fws=0&ohw=0&ga_vid=1969059549.1675822065&ga_sid=1675822065&ga_hid=544952119&ga_fc=false	false		high
http://https://pixel-eu.onaudience.com/?partner=270&smartmap=1&gdpr=0&gdpr_consent=&redirect=image2.pubmatic.com%2FAdServer%2FPug%3Fvcode%3Dbz0yJnR5cGU9MSZjb2RlPTI4ODQmdGw9MTI5NjAw%26piggybackCookie%3D%25_rid%26gdpr%3D0%26gdpr_consent%3D%25_gdpr_consent	false	• Avira URL Cloud: safe	unknown
http://https://cm.g.doubleclick.net/pixel?google_nid=triplelift&gdpr=0&gdpr_consent=&us_privacy=&google_hm=NDI1OTQzMDk3NTY0NTI4NTAzMDUxOA%3D%3D	false		high
http://https://a.audrte.com/p	false	• Avira URL Cloud: safe	unknown
http://https://sync.1rx.io/usersync2/rmphb?zcc=1&redir=https%3A%2F%2Fprebid.tpdads.com%2Fsetuid%3Fbidder%3Dunruly%26gdpr%3D%26gdpr_consent%3D%26f%3Di%26uid%3D%5BRX_UUID%5D&cb=1675789694743	false		high
http://https://securepubads.g.doubleclick.net/gampad/ads?pvsid=4287636170759586&correlator=3848810272311789&eid=31072031%2C31072039&output=ldjh&gdfp_req=1&vrg=2023020201&ptt=17&impl=fif&iu_parts=134702932%2C0337-familyproof.com%2C0337-dsk-banner-ad-d&enc_prev_ius=%2F0%2F1%2F2&prev_iu_szs=970x250%7C970x90%7C728x90%7C468x60&ifi=4&adks=3786041093&sfv=1-0-40&prev_scp=position%3Ddsk-banner-ad-d%26refreshcount%3D1%26refresh%3Dfalse%26amznbid%3D1%26amznp%3D1%26optimera%3DZ%2C20%2CD4%2CM6%2CE1%2CM7%2CM1%2CJ0%2CDE%2CA%2CLA_709%2CLA_711%2CLA_713%2CLA_714%2CLA_720%2CLA_724%2CLA_727%2CLA_740%2CLA_754%2CLA_755%2CLA_757%2CLB_710%2CLB_712%2CLB_719%2CLB_742%2CLB_756%2CLB_758%2CLB_759%2CLB_760&eri=1&cust_params=domain%3Dfamilyproof.com%26Page-Type%3Dhome%26URL%3Dhttps%253A%252F%252Fwww.familyproof.com%252F%26session_id%3DU1dwherEdbke76Q%26path%3D%252F%26url%3D%252F%26kw%3DFamilyProof%252C%257C%252CTips%252C%252CAnswers%252C%2526%252CAdvice&sc=1&cookie=ID%3De865e957478f33a0-2220b777e9da0015%3AT%3D1675789665%3ART%3D1675789665%3AS%3DALNI_MZ7qAbgfbuZ3Skh2x9KZ9GpQbihDA&gpic=UID%3D00000bb1552dc58c%3AT%3D1675789665%3ART%3D1675789665%3AS%3DALNI_MYUho0SSsKXSuGrPy5e7JP866nApA&abxe=1&dt=1675822078657&lmt=1675822078&dlt=1675822060272&idt=4785&adxs=147&adys=2234&biw=1263&bih=913&scr_x=0&scr_y=0&btvi=1&ucis=3&oid=2&u_his=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_sd=1&u_tz=-480&dmc=8&bc=31&uach=WyJXaW5kb3dzIiwiNi4wLjAiLCJ4ODYiLCIiLCIxMDQuMC41MTEyLjgxIixbXSxmYWxzZSxudWxsLCI2NCIsW1siQ2hyb21pdW0iLCIxMDQuMC41MTEyLjgxIl0sWyIgTm90IEE7QnJhbmQiLCI5OS4wLjAuMCJdLFsiR29vZ2xlIENocm9tZSIsIjEwNC4wLjUxMTIuODEiXV0sZmFsc2Vd&nvt=1&url=https%3A%2F%2Fwww.familyproof.com%2F&frm=20&vis=1&psz=1150x162&msz=1078x90&fws=0&ohw=0&ga_vid=1969059549.1675822065&ga_sid=1675822065&ga_hid=544952119&ga_fc=false	false		high
http://https://green.erne.co/pubmatic/cm?gdpr=0&gdpr_consent=	false		high
http://https://image6.pubmatic.com/AdServer/PugMaster?sec=1&async=1&kdntuid=1&rnd=51596895&p=156011&s=165626&a=0&ptask=ALL&np=0&fp=0&rp=0&mpc=0&spug=1&coppa=0&gdpr=0&gdpr_consent=&us_privacy=	false		high
http://https://g2.gumgum.com/hbid/imp?lt=1675822065261&to=480&aun=dsk-banner-ad-d&t=0ed7c58f&pi=3&maxw=970&maxh=250&si=945924&bf=970x250%2C970x90%2C728x90%2C468x60&schain=1.0%2C1!publisherdesk.com%2C100337%2C1%2C%2C%2C&vw=1280&vh=913&sw=1280&sh=1024&pu=https%3A%2F%2Fwww.familyproof.com%2F&ce=true&dpr=1&jcsi=%7B%22t%22%3A0%2C%22rq%22%3A8%2C%22pbv%22%3A227.32.0%22%7D&ogu=https%3A%2F%2Fwww.familyproof.com%2F&ns=10138	false		high
http://https://aax-eu.amazon-adsystem.com/s/ecm3?id=GHiktPZHKozKZ33vQ4GvdgIx&ex=sovrn.com&gdpr=0&gdpr_consent=	false		high

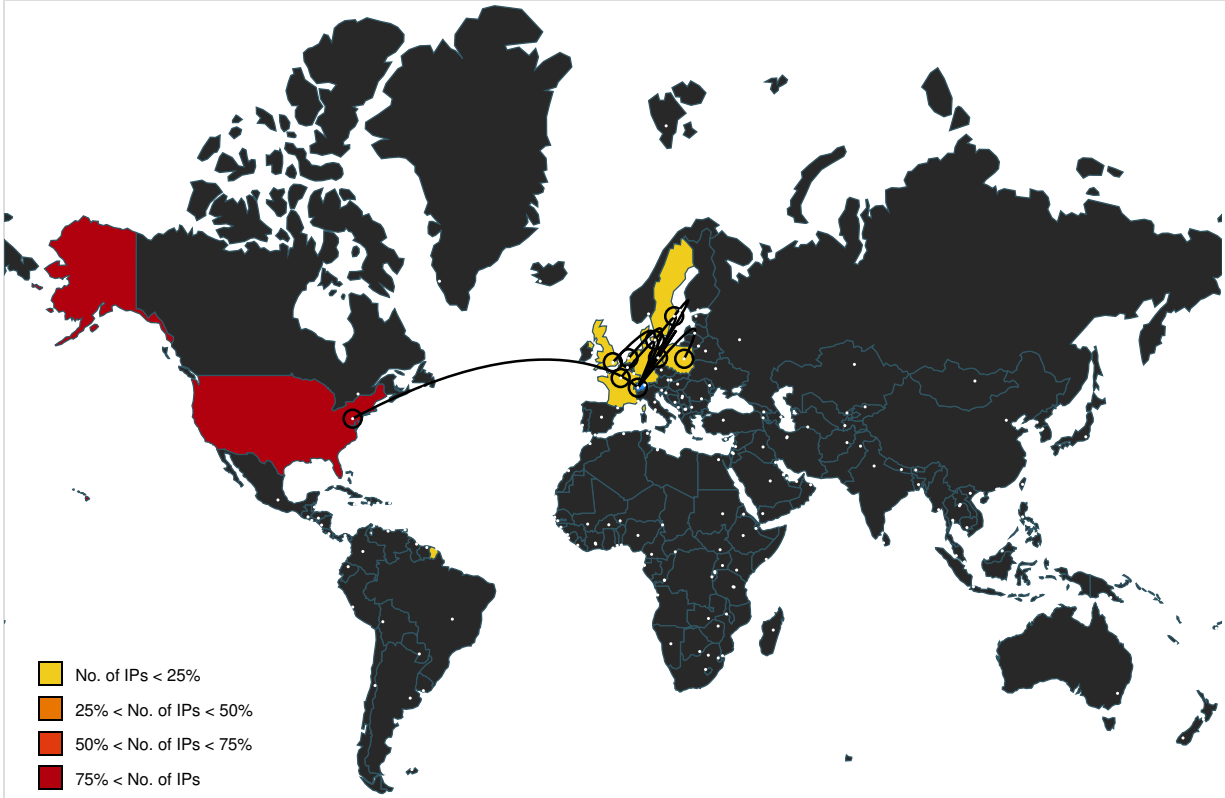
Name	Malicious	Antivirus Detection	Reputation
http://https://g2.gumgum.com/hbid/imp?lt=1675822065249&to=480&aun=dsk-banner-ad-a&t=0ed7c58f&pi=3&maxw=970&maxh=90&si=945926&bf=970x90%2C728x90%2C468x60%2C320x50%2C300x100%2C300x50%2C1x1&schain=1.0%2C1!publisherdesk.com%2C100337%2C1%2C%2C%2C&vw=1280&vh=913&sw=1280&sh=1024&pu=https%3A%2F%2Fwww.familyproof.com%2F&ce=true&dpr=1&jcsi=%7B%22t%22%3A0%2C%22rq%22%3A8%2C%22pbv%22%3A%227.32.0%22%7D&ogu=https%3A%2F%2Fwww.familyproof.com%2F&ns=10138	false		high
http://https://sync.mathtag.com/sync/img?mt_exid=5&redir=https%3A%2F%2Feu-u.openx.net%2Fw%2F1.0%2Fsd%3Fid%3D536872786%26val%3D%5BMM_UUID%5D	false		high
http://https://ap.lijit.com/beacon/amazon?url=https://aax-eu.amazon-adsystem.com%2Fs/ecm3?id=$UID&ex=sovrn.com&dnr=1	false		high
http://https://aax-eu.amazon-adsystem.com/x/px/JKlc_E30RxHrDvVAJVrpXxEAAAGGLNk5NwMAAAJYAQBhcHNfdHhuX2JpZDEgICBOL0EgICAgICAgICAgICCF6U5X/v/%7B%22v%22:%7B%22p%22:100,%22t%22:1,%22def%22:%22groupm%22%7D,%22vs%22:%22visible%22,%22ah%22:90,%22aw%22:728,%22ttv%22:3.86,%22ts%22:1675822101845,%22bn%22:false,%22pixelId%22:%22gsn4veez8kp%22,%22ver%22:%22r-1.30%22%7D?cb=8968782	false		high
http://https://prebid.a-mo.net/cchain/0?gdpr=&us_privacy=&cb=https%3A%2F%2Fprebid.tpdads.com%2Fsetuid%3Fbidder%3Damx%26gdpr%3D%26gdpr_consent%3D%26f%3Di%26uid%3D	false	• Avira URL Cloud: safe	unknown
http://https://image4.pubmatic.com/AdServer/SPug?partnerID=156078&xid=y-XNFaGNBE2uUcBNPIL762z6jmEUyLg8Y-~A&gdpr=0	false		high
http://https://eb2.3lift.com/xuid?mid=2409&xuid=5d8a3476-cd27-4aa7-a732-82e8bd53a2ec&dongle=d3d3&gdpr=&gdpr_consent=&gdpr_pd=	false		high
http://https://pixel-sync.sitescout.com/dmp/pixelSync?cookieQ=1&nid=3&gdpr=0&gdpr_consent=	false		high
http://https://aax.amazon-adsystem.com/x/px/JAlgBUvUkfUi3o4dqz00pbcAAAGGLNk5OAMAAAJYAQBhcHNfdHhuX2JpZDEgICBOL0EgICAgICAgICBe71VB/%7B%22adCsm%22:[%7B%22tld%22:%22www.familyproof.com%22%7D,%7B%22vfrd%22:4,%22dbg%22:%22nomime%22%7D,%7B%22ns%22:1675822084728,%22st%22:%222805.20%22,%22re%22:%229281.40%22,%22ldTot%22:%226476.20%22%7D,%7B%22lteu%22:%220.20%22,%22ltut%22:%220.00%22,%22ltpq%22:%220.00%22,%22lths%22:%220.00%22,%22ltpm%22:%220.00%22,%22ltdm%22:%220.30%22,%22ltdb%22:%220.00%22,%22csmTot%22:%221.00%22%7D],%22pixelId%22:%22xgmjvgutng9%22,%22ts%22:1675822096566,%22ver%22:%22d-1.20%22%7D?cb=3207108	false		high
http://https://dyv1bugovvq1g.cloudfront.net/68/www.familyproof.com/.js	false		high
http://https://aax-eu.amazon-adsystem.com/e/dtb/imp?b=JH0OtCYu__BOdhleQsZAe8oAAAGGLNk5OAMAAAJYAQBhcHNfdHhuX2JpZDEgICBOL0EgICAgICAgICAgICCvyO4R&pp=srvpxc&isip=1&vi=1	false		high
http://https://match.adsrvr.org/track/rid?ttd_pid=pubmatic&fmt=json	false		high
http://https://cdn.ampproject.org/rtv/012301242213000/v0/amp-analytics-0.1.mjs	false		high
http://https://cm.g.doubleclick.net/pixel?google_nid=rubicon&google_hm=ZTBjYjI0OGY4OTgyYmYzN2Q5ZDRiODc1ZjNiZDMwN2Q4MDA0YTIxNg	false		high
http://https://simage2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZqcz0xJmNvZGU9Mjk0NSZ0bD0xMjk2MDA=&piggybackCookie=5d8a3476-cd27-4aa7-a732-82e8bd53a2ec&gdpr=0&gdpr_consent=&gdpr_pd=	false		high
http://https://contextual.media.net/cksync.php?cs=3&type=yld&ovsid=setstatuscode&redirect=https%3A%2F%2Fads.yieldmo.com%2Fv000%2Fsync%3Fpn_id%3Dmnt%26userid%3D%3Cvsid%3E	false		high
http://https://sync.srv.stackadapt.com/sync?nid=21	false		high
http://https://www.familyproof.com/wp-content/uploads/2023/01/brooke-lark-jUPOXXRNdcA-unsplash-788x444.jpg	false	• Avira URL Cloud: safe	unknown
http://https://aax-eu.amazon-adsystem.com/e/dtb/admi?b=JKlc_E30RxHrDvVAJVrpXxEAAAGGLNk5NwMAAAJYAQBhcHNfdHhuX2JpZDEgICBOL0EgICAgICAgICAgICCF6U5X&rnd=629611027751167582208530 9&pp=6ks7b4&p=fnwwlc&crid=50024435&ep=%7B%22ce%22%3A%221%22%7D	false		high
http://https://simage2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTc4JnRsPTE1NzY4MDA=&piggybackCookie=582804750717643 6426&gdpr=0&gdpr_consent=	false		high
http://https://get.geojs.io/v1/ip/country.json	false	• Avira URL Cloud: safe	unknown
http://https://aax-eu.amazon-adsystem.com/s/ecm3?ex=media.net&id=3187912931358142000V10	false		high
http://https://prebid.tpdads.com/setuid?bidder=medianet&gdpr=&gdpr_consent=&f=i&uid=0000EEA	false	• Avira URL Cloud: safe	unknown
http://https://www.familyproof.com/wp-includes/js/jquery/jquery.min.js?ver=3.6.1	false	• Avira URL Cloud: safe	unknown
http://https://cdn.parsely.com/keys/familyproof.com/p.js?ver=3.6.1	false		high
http://https://www.familyproof.com/	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://securepubads.g.doubleclick.net/gampad/ads?pvsid=4287636170759586&correlator=3848810272311789&eid=31072031%2C31072039&output=ldjh&gdfp_req=1&vrg=2023020201&ptt=17&impl=fif&iu_parts=134702932%2C0337-familyproof.com%2C0337-dsk-banner-ad-c&enc_prev_ius=%2F0%2F1%2F2&prev_iu_szs=320x50%7C970x250%7C970x90%7C728x90%7C468x60%7C1x1&fluid=height&ifi=8&adks=1211506645&sfv=1-0-40&prev_scp=position%3Ddsk-banner-ad-c%26refreshcount%3D1%26refresh%3Dfalse%26amznbid%3D1%26amznp%3D1%26optimera%3DZ%2C10%2CF5%2CD4%2CE1%2CM7%2CJ0%2CDE%2CA%2CLA_709%2CLA_711%2CLA_713%2CLA_714%2CLA_720%2CLA_724%2CLA_727%2CLA_740%2CLA_754%2CLA_755%2CLA_757%2CLB_710%2CLB_712%2CLB_719%2CLB_742%2CLB_756%2CLB_758%2CLB_759%2CLB_760&eri=1&cust_params=domain%3Dfamilyproof.com%26PageType%3Dhome%26URL%3Dhttps%253A%252F%252Fwww.familyproof.com%252F%26session_id%3DU1dwherEdbke76Q%26path%3D%252F%26url%3D%252F%26kw%3DFamilyProof%252C%257C%252CTips%252C%252CAnswers%252C%2526%252CAdvice&sc=1&cookie=ID%3De865e957478f33a0-2220b777e9da0015%3AT%3D1675789665%3ART%3D1675789665%3AS%3DALNI_MZ7qAbgfbuZ3Skh2x9KZ9GpQbihDA&gpic=UID%3D00000bb1552dc58c%3AT%3D1675789665%3ART%3D1675789665%3AS%3DALNI_MYUho0SSsKXSuGrPy5e7JP866nApA&abxe=1&dt=1675822078790&lmt=1675822078&dlt=1675822060272&idt=4785&adxs=147&adys=1219&biw=1263&bih=913&scr_x=0&scr_y=0&btvi=2&ucis=7&oid=2&u_his=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_sd=1&u_tz=-480&dmc=8&bc=31&uach=WyJXaW5kb3dzIiwiNi4wLjAiLCJ4ODYiLCIiLCIxMDQuMC41MTEyLjgxIixbXSxmYWxzZSxudWxsLCI2NCIsW1siQ2hyb21pdW0iLCIxMDQuMC41MTEyLjgxIl0sWyIgTm90IEE7QnJhbmQiLCI5OS4wLjAuMCJdLFsiR29vZ2xlIENocm9tZSIsIjEwNC4wLjUxMTIuODEiXV0sZmFsc2Vd&nvt=1&url=https%3A%2F%2Fwww.familyproof.com%2F&frm=20&vis=1&psz=1150x162&msz=1078x90&fws=0&ohw=0&ga_vid=1969059549.1675822065&ga_sid=1675822065&ga_hid=544952119&ga_fc=false	false		high
http://https://cm.g.doubleclick.net/pixel?google_nid=pubmatic&google_cm&google_sc&gdpr=0&gdpr_consent=	false		high
http://https://ssbsync.smartadserver.com/api/sync?callerId=43&gdpr=0&gdpr_consent=	false		high
http://https://www.familyproof.com/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://hb.undertone.com/hb?pid=2981&domain=familyproof.com	false		high
http://https://securepubads.g.doubleclick.net/pagead/adview?ai=CsFA2b4XiY6fPltK99u8PhJGN-A_q3Mr5XLbvqsNNwI23ARABIABguwaCARdjYS1wdWltMjMyMjE1Nzg2OTYwOTQ0OcgBCeACAKgDAaoEgAJP0GCiFYHZWMasp7tK53r2fsklx3a0gVpcZVQ1whlplKU6CkI7RZ8eMLoXOtxBFfoQVzhItgIliznnUSCfuJHwORvx_s02vaMv5Rp480KLPpAWNaRQ_clw--eH3bTieoBg21_TczwS56etqShVm-joLD8wzrRZUdEQBvVAEGLgfnReBZQ8Go8__XOYjVZMf30dNHD6X8fAPxzBtXGeB-i_YNufjM4TEw4t1sXsSE3ql4jwio0Epe1P70zDkTMZEd4ZXtNvJiDA-OhBqobkcNOfGCARusNj2wsKS_XE71snRuOBsi3mPK3XaiycFZoB-63lJgGVKKKhQEQvIFC1scMW4AQBgAaK4b-rg47D7QmgBiGoB6a-G6gHltgbqAeqm7ECqAf_nrECqAffn7EC2AcA0ggPCIDhgBAQATICqgI6AoBAgAoD-gsCCAGADAHQFQGAFwGyFxwKGhIUcHViLTIzMjIxNTc4Njk2MDk0NDkY_MgX&sigh=eA_qadyd8eY&uach_m=[UACH]&cid=CAQSPADUE5ym4kYBSPt4kRMw5wqsufIF7EnBVpNfoWLsYNzbrG6n75bUAnZOlS6T1SYu5o-RM8a78jxDktJ0ThgB	false		high
http://https://g2.gumgum.com/hbid/imp?lt=1675822123175&to=480&aun=dsk-banner-ad-a&criteoId=qXfxHl9VSiUyRmx5anUlMkZLUW8lMkZEU0c5TW9tV3k0cnE5czIwcE1ocDFqMkMlMkZBaElzemRRWm51QjZ1JTJGNmp0MnFyUUNUQXFlaSUyRmtMJTJCeXRBalFkTllGTWxTWTI3clRRJTNEJTNE&id5id=0&pubcid=b2844ada-ab41-4456-ac98-1839b08794a2&pv=4f0e54de-cc91-49b1-80b0-ada2cac20de2&fp=0.25&fpc=USD&t=0ed7c58f&pi=3&maxw=970&maxh=90&si=945929&bf=970x90%2C728x90%2C468x60%2C320x50%2C300x100%2C300x50%2C1x1&schain=1.0%2C1!publisherdesk.com%2C100337%2C1%2C%2C%2C&vw=1280&vh=913&sw=1280&sh=1024&pu=https%3A%2F%2Fwww.familyproof.com%2F&ce=true&dpr=1&jcsi=%7B%22t%22%3A0%2C%22rq%22%3A8%2C%22pbv%22%3A%227.32.0%22%7D&ogu=https%3A%2F%2Fwww.familyproof.com%2F&ns=5734	false		high
http://https://idsync.frontend.weborama.fr/ids?key=pubmatic&value=18087908-2EE2-43CE-BDCD-C14DA8DE6120	false		high
http://https://www.familyproof.com/wp-content/uploads/2023/01/child_boy_game_package_box_kid_gift_moving_to-917512-788x444.jpg	false	• Avira URL Cloud: safe	unknown
http://https://aax.amazon-adsystem.com/x/px/JH0OtCYu__BOdhleQsZAe8oAAAGGLNk5OAMAAAJYAQBhcHNfdHhuX2JpZDEgICBOL0EgICAgICAgICAgICCvyO4R/%7B%22adCsm%22:[%7B%22tld%22:%22www.familyproof.com%22%7D,%7B%22vfrd%22:4,%22dbg%22:%22nomime%22%7D,%7B%22ns%22:1675822084210,%22st%22:%221339.80%22,%22re%22:%221844.60%22,%22ldTot%22:%22504.80%22%7D,%7B%22lteu%22:%220.10%22,%22ltut%22:%220.00%22,%22ltpq%22:%220.00%22,%22lths%22:%220.20%22,%22ltpm%22:%220.30%22,%22ltdm%22:%220.40%22,%22ltdb%22:%220.00%22,%22csmTot%22:%221.50%22%7D],%22pixelId%22:%22nca75uldew%22,%22ts%22:1675822094705,%22ver%22:%22d-1.20%22%7D?cb=1371933	false		high
http://https://cm.g.doubleclick.net/pixel?google_nid=zeotap_ddp&google_cm&zpartnerid=1&env=mWeb&eventType=map&id_mid_4=89a8e2dd-3372-4140-5da6-cdcc11a6daaa&reqId=7281fea6-6124-4968-58ad-361623423691&zcluid=44e36b010bef0590&zdid=1332	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://securepubads.g.doubleclick.net/gampad/ads?pvsid=4287636170759586&correlator=2034456303232831&eid=31072031%2C31072039&output=ldjh&gdfp_req=1&vrg=2023020201&ptt=17&impl=fif&iu_parts=134702932%2C0337-familyproof.com-oop%2C0337-peel&enc_prev_ius=%2F0%2F1%2F2&prev_iu_szs=336x280%7C300x250&ifi=9&adks=2794714471&sfv=1-0-40&ris=2&rcs=1&prev_scp=position%3Doop-ad-b%26refreshcount%3D1%26refresh%3Dfalse%26optimera%3DZ%2C70%2CA6%2CJ1%2CDE%2CA%2CLA_709%2CLA_711%2CLA_713%2CLA_714%2CLA_720%2CLA_724%2CLA_727%2CLA_740%2CLA_754%2CLA_755%2CLA_757%2CLB_710%2CLB_712%2CLB_719%2CLB_742%2CLB_756%2CLB_758%2CLB_759%2CLB_760&eri=1&cust_params=domain%3Dfamilyproof.com%26PageType%3Dhome%26URL%3Dhttps%253A%252F%252Fwww.familyproof.com%252F%26session_id%3DU1dwherEdbke76Q%26path%3D%252F%26url%3D%252F%26kw%3DFamilyProof%252C%257C%252CTips%252C%252CAnswers%252C%2526%252CAdvice&sc=1&cookie=ID%3De865e957478f33a0-2220b777e9da0015%3AT%3D1675789665%3AS%3DALNI_MZ7qAbgfbuZ3Skh2x9KZ9GpQbihDA&gpic=UID%3D00000bb1552dc58c%3AT%3D1675789665%3ART%3D1675789665%3AS%3DALNI_MYUho0SSsKXSuGrPy5e7JP866nApA&abxe=1&dt=1675822080546&lmt=1675822080&dlt=1675822060272&idt=4785&adxs=-12245933&adys=-12245933&biw=1263&bih=913&scr_x=0&scr_y=0&btvi=-1&ucis=1&oid=2&u_his=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_sd=1&u_tz=-480&dmc=8&bc=31&uach=WyJXaW5kb3dzIiwiNi4wLjAiLCJ4ODYiLCIiLCIxMDQuMC41MTEyLjgxIixbXSxmYWxzZSxudWxsLCI2NCIsW1siQ2hyb21pdW0iLCIxMDQuMC41MTEyLjgxIl0sWyIgTm90IEE7QnJhbmQiLCI5OS4wLjAuMCJdLFsiR29vZ2xlIENocm9tZSIsIjEwNC4wLjUxMTIuODEiXV0sZmFsc2Vd&nvt=1&url=https%3A%2F%2Fwww.familyproof.com%2F&frm=20&vis=1&psz=58x-1&msz=0x-1&fws=640&ohw=0&ga_vid=1969059549.1675822065&ga_sid=1675822065&ga_hid=544952119&ga_fc=false	false		high
http://https://sync.richaudience.com/74889303289e27f327ad0c6de7be7264/?p=1BTOoaD22a&r=https%3A%2F%2Fu.4dex.io%2Fsetuid%3Fbidder%3Drichaudience%26uid%3D[PDID]	false		high
http://https://g2.gumgum.com/hbid/imp?lt=1675822065263&to=480&aun=dsk-banner-ad-d&t=0ed7c58f&pi=3&maxw=970&maxh=250&si=945926&bf=970x250%2C970x90%2C728x90%2C468x60&schain=1.0%2C1!publisherdesk.com%2C100337%2C1%2C%2C%2C&vw=1280&vh=913&sw=1280&sh=1024&pu=https%3A%2F%2Fwww.familyproof.com%2F&ce=true&dpr=1&jcsi=%7B%22t%22%3A0%2C%22rq%22%3A8%2C%22pbv%22%3A227.32.0%22%7D&ogu=https%3A%2F%2Fwww.familyproof.com%2F&ns=10138	false		high
http://https://u.4dex.io/setuid?bidder=indexexchange&uid=Y-KFdBYMDP6MQHUBZ5vSBQAABIUAAAAB	false	• Avira URL Cloud: safe	unknown
http://https://b1t-eudc1.zemanta.com/t/imp/view/SE3B5CFDHJV7VS4PBTXJ5SBXAI63NRQTBXHFOKV7Q4YTGU2M5ESIIA5OLSNG26LTHMZNZIKKLLMXHAT52FEWSO37WSPWSB5SBJM4BP4NUY5B6Z5GZGYH5WUBU2M2LDKVWYMZUHDPKMWLM376QF7GEOR25BWSFUXTHLK2FNL6V6FE454O2UVGLLEPUDIHPCQF3LLZU67CVK2INC3677XEIRYKPU5HO6IYBKIJCQ74ML4M4W6XCR3S72PNRNTTFIFQUZR7GDWBNBZZVRBMSXQOLCVO4UMSCNYFMDJCLKFJSMEQBH5GKNG62RYV5AJZXA7UXALPLRKWV6SGKX5ICQCFHZJPDUYL2HVGWNU6QOGJAU33Q4O5UVWX7IMA4F5A54TH/?	false		high
http://https://ssc-cms.33across.com/ps/?m=xch&rt=html&id=0015a00002oUk4aAAC&ru=https%3A%2F%2Fu.4dex.io%2Fsetuid%3Fbidder%3D33across%26uid%3D33XUSERID33X	false		high
http://https://prebid.tpdads.com/openrtb2/auction	false	• Avira URL Cloud: safe	unknown
http://https://aax-eu.amazon-adsystem.com/x/px/JAlgBUvUkfUi3o4dqz00pbcAAAGGLNk5OAMAAAJYAQBhcHNfdHhuX2JpZDEgICBOL0EgICAgICAgICAgICBe71VB/atf/%7B%22atf%22:true,%22f%22:1,%22vs%22:%22visible%22,%22ah%22:90,%22aw%22:728,%22ts%22:1675822100730,%22bn%22:false,%22pixelId%22:%229b85yzpryaw%22,%22ver%22:%22r-1.30%22%7D?cb=1684905	false		high
http://https://cm-supply-web.gammaplatform.com/adx/usersyncsupply?pid=7&t=pixel	false		high
http://https://aax-eu.amazon-adsystem.com/x/px/JOfPmxRSeY2WNIeoWhUGCgUAAAGGLNnoCwMAAAJYAQBhcHNfdHhuX2JpZDEgICBOL0EgICAgICAgICBmNDcQ/%7B%22adCsm%22:[%7B%22ns%22:1675822134928,%22st%22:%2294.10%22,%22re%22:%2294.10%22,%22ldTot%22:%220.00%22%7D,%7B%22lteu%22:%220.10%22,%22ltut%22:%220.00%22,%22ltpq%22:%220.00%22,%22csmTot%22:%229.00%22%7D],%22pixelId%22:%223oectrimmgo%22,%22ts%22:1675822138835,%22ver%22:%22r-1.30%22%7D?cb=9301017	false		high
http://https://x.bidswitch.net/check_uuid/https%3A%2F%2Faax-eu.amazon-adsystem.com%2Fs%2Fecm3%3Fex%3Dmediagrid.com%26id%3D%24%7BBSW_UUID%7D	false	• Avira URL Cloud: safe	unknown
http://https://cm.g.doubleclick.net/pixel?google_nid=pmeb&google_sc=1&google_hm=GAh5CC7iQ869zcFNqN5hIA%3D%3D&gdpr=0&gdpr_consent=	false		high
http://https://ce.lijit.com/merge?pid=92&3pid=5828047507176436426&gdpr=0&gdpr_consent=	false		high
http://https://cm.g.doubleclick.net/pixel?google_nid=rubicon&google_cm&google_sc	false		high
http://https://aax-eu.amazon-adsystem.com/s/ecm3?ex=smaato.com&id=541aea9	false		high
http://https://simage2.pubmatic.com/AdServer/Pug?gdpr_consent=&gdpr=0&piggybackCookie=uid:bae997af-cc04-47f2-ad11-ee997237f53e&vcode=bz0yJnR5cGU9MSZjb2RlPTMwNjImdGw9MTI5NjAw	false		high
http://https://cdn.p-n.io/pushly-sdk.min.js?domain_key=tuYtwQ25XFtJZbspIunR6b5BjhiurM3ckeEC&ver=6.1.1	false	• Avira URL Cloud: safe	unknown
http://https://sync.mathtag.com/sync/img?mt_exid=3&gdpr=0&gdpr_consent=&redir=https%3A%2F%2Fsimage2.pubmatic.com%2FAdServer%2FPug%3Fvcode%3Dbz0yJnR5cGU9MSZjb2RlPTM2MiZ0bD0xMjk2MDA%3D%3D%26piggybackCookie%3Duid%3A%5BMM_UUID%5D	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://rtb.mfadsrvr.com/ul_cb/sync?ssp=yieldmo	false	• Avira URL Cloud: safe	unknown
http://https://ib.adnxs.com/bounce?%2Fgetuid%3Fhttps%253A%252F%252Fprebid.tpdads.com%252Fsetuid%253Fbidder%253Dadnxs%2526gdpr%253D%2526gdpr_consent%253D%2526f%253Di%2526uid%253D%2524UID	false		high
http://https://s.amazon-adsystem.com/dcm?pid=78af914c-e755-4b90-bded-1b172aedc763&us_privacy=&gdpr=&gdpr_consent=&id=Y-KFdBYMDP6MQHUBZ5vSBQAABIUAAAAB	false		high
http://https://www.familyproof.com/wp-content/mu-plugins/tpd-featured-posts/src/slick-carousel/slick.min.js?ver=1.8.1	false	• Avira URL Cloud: safe	unknown
http://https://image6.pubmatic.com/AdServer/PugMaster?sec=1&async=1&kdntuid=1&rnd=67306210&p=159110&s=0&a=0&ptask=ALL&np=0&fp=0&rp=0&mpc=0&spug=1&coppa=0&gdpr=0&gdpr_consent=&us_privacy=	false		high
http://https://aax-eu.amazon-adsystem.com/e/dtb/imp?b=JOfPmxRSeY2WNIeoWhUGCgUAAAGGLNnoCwMAAAJYAQBhcHNfdHhuX2JpZDEgICBOL0EgICAgICAgICAgICBmNDcQ&pp=1num8sg&isip=1&vi=1	false		high
http://https://eu-u.openx.net/w/1.0/sd?id=536872786&val=efad63e2-8571-4f00-8c7b-7c718902bd13	false		high
http://https://www.google.com/pagead/drt/ui	false		high
http://https://k.p-n.io/event-stream	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
147.75.85.234	prebid.a-mo.net	Switzerland		54825	PACKETUS	false
142.250.180.129	cdn-content.ampproject.org	United States		15169	GOOGLEUS	false
98.98.134.241	pixel-a.sitescout.com	United States		7018	ATT-INTERNET4US	false
104.18.24.173	s.tribalfusion.com	United States		13335	CLOUDFLARENETUS	false
216.52.2.30	unknown	United States		29791	VOXEL-DOT-NETUS	false
216.58.209.45	accounts.google.com	United States		15169	GOOGLEUS	false
2.18.160.23	hbx.media.net	European Union		16625	AKAMAI-ASUS	false
169.63.109.126	in-appadvertising.com	United States		36351	SOFTLAYERUS	false
185.64.190.81	spug-lhrc.pubmnet.com	United Kingdom		62713	AS-PUBMATICUS	false
142.251.209.34	www.googletagservices.com	United States		15169	GOOGLEUS	false
18.195.181.132	match-eu-central-1-ecs.sharethrough.com	United States		16509	AMAZON-02US	false
68.67.179.153	nym1-ib.adnxs.com	United States		29990	ASN-APPNEXUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.76.46.33	g2.gumgum.com	United States		16509	AMAZON-02US	false
146.75.122.132	outbrain.map.fastly.net	Sweden		30051	SCCGOVUS	false
91.228.74.206	global.px.quantserve.com	United Kingdom		27281	QUANTCASTUS	false
3.215.74.86	1x1.a-mo.net	United States		14618	AMAZON-AESUS	false
178.250.2.151	widget.am5.vip.prod.criteo.com	France		44788	ASN-CRITEO-EUROPEFR	false
141.94.170.64	pixel.onaudience.com	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
13.248.245.213	eu-eb2.3lift.com	United States		16509	AMAZON-02US	false
13.224.89.76	d1jvc9b8z3vcjs.cloudfront.net	United States		16509	AMAZON-02US	false
132.226.41.106	unknown	United States		16989	UTMEMUS	false
185.86.138.151	ssbsync-itx5.smartadserver.com	France		201081	SMARTADSERVERFR	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
185.89.211.84	ib.anycast.adnxs.com	Germany		29990	ASN-APPNEXUS	false
142.251.209.1	pagead-googlehosted.l.google.com	United States		15169	GOOGLEUS	false
104.21.30.178	cdn.optmn.cloud	United States		13335	CLOUDFLARENETUS	false
34.250.26.242	unknown	United States		16509	AMAZON-02US	false
67.202.105.22	pixel.33across.com	United States		32748	STEADFASTUS	false
13.224.98.168	dgcbxsxpz6nta.cloudfront.net	United States		16509	AMAZON-02US	false
142.250.180.130	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
162.19.80.91	bl1-eu.dyntrk.com	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
52.94.223.37	aax-eu.amazon-adsystem.com	United States		16509	AMAZON-02US	false
185.255.84.153	visitor-fra02.omnitagjs.com	France		200271	IGUANE-FR	false
54.78.254.47	load-euw1.exelator.com	United States		16509	AMAZON-02US	false
141.94.171.214	pixel-eu.onaudience.com	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
104.18.2.114	mp.4dex.io	United States		13335	CLOUDFLARENETUS	false
178.250.2.146	gum.am5.vip.prod.criteo.com	France		44788	ASN-CRITEO-EUROPEFR	false
185.80.39.216	fr-xn.lb.indexww.com	Netherlands		27381	CASALE-MEDIACA	false
52.209.237.217	protected-by.clarium.io	United States		16509	AMAZON-02US	false
162.19.138.120	id5-sync.com	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
185.64.189.110	pug22000nfc.pubmnet.com	United Kingdom		62713	AS-PUBMATICUS	false
104.22.25.87	mwzeom.zeotap.com	United States		13335	CLOUDFLARENETUS	false
54.199.165.234	cc.adingo.jp	United States		16509	AMAZON-02US	false
159.65.194.197	match.adsby.bidtheatre.com	United States		14061	DIGITALOCEAN-ASNUS	false
52.73.105.161	a.audrte.com	United States		14618	AMAZON-AESUS	false
150.136.156.92	adserver.technoratimedia.com	United States		31898	ORACLE-BMC-31898US	false
185.89.211.12	unknown	Germany		29990	ASN-APPNEXUS	false
213.155.156.165	d5p.de17a.com	European Union		1299	TELIANETTeliaCarrierEU	false
104.22.7.45	prebidtest.zemanta.com	United States		13335	CLOUDFLARENETUS	false
216.52.2.48	oeu.vap.lijit.com	United States		29791	VOXEL-DOT-NETUS	false
104.18.17.107	cdn.confiant-integrations.net	United States		13335	CLOUDFLARENETUS	false
3.125.220.90	btlr-ecs-eu-central-1.sharethrough.com	United States		16509	AMAZON-02US	false
34.120.133.55	api.rlcdn.com	United States		15169	GOOGLEUS	false
185.64.190.78	pugm-lhrc.pubmnet.com	United Kingdom		62713	AS-PUBMATICUS	false
141.95.97.230	ws.rqtrk.eu	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
104.26.9.169	script.4dex.io	United States		13335	CLOUDFLARENETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.70.233	get.geojs.io	United States		13335	CLOUDFLARENETUS	false
157.90.40.26	matching.truffle.bid	United States		766	REDIRISRedIRISAutonomousSystemES	false
35.201.96.126	visitor.fiftyt.com	United States		15169	GOOGLEUS	false
185.64.189.229	aud-amsc.pubmnet.com	United Kingdom		62713	AS-PUBMATICUS	false
3.122.24.207	alb-aws-fr-bruges-1875226813.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
35.190.0.66	ads.travelaudience.com	United States		15169	GOOGLEUS	false
104.18.25.173	a.tribalfusion.com	United States		13335	CLOUDFLARENETUS	false
3.236.169.43	queue.amazonaws.com	United States		14618	AMAZON-AESUS	false
63.34.81.234	p1.parsely.com	United States		16509	AMAZON-02US	false
35.214.223.115	envoy1.envoy-csync1.core-b8mf.ov1o.com	United States		19527	GOOGLE-2US	false
13.224.98.18	dyv1bugovvq1g.cloudfront.net	United States		16509	AMAZON-02US	false
35.244.193.51	lexicon.33across.com	United States		15169	GOOGLEUS	false
52.46.128.147	s.amazon-adsystem.com	United States		16509	AMAZON-02US	false
165.227.249.173	prebid.tpdads.com	United States		14061	DIGITALOCEAN-ASNUS	false
18.159.168.223	k.p-n.io	United States		16509	AMAZON-02US	false
77.243.60.138	uip.semasio.net	Denmark		42697	NETIC-ASDK	false
54.194.53.119	sync.crwdcntrl.net	United States		16509	AMAZON-02US	false
52.220.229.2	cm-supply-web.gammaplatform.com	United States		16509	AMAZON-02US	false
52.0.142.7	sync.srv.stackadapt.com	United States		14618	AMAZON-AESUS	false
185.183.112.148	sync.adotmob.com	Netherlands		60350	VPFR	false
142.250.180.166	ad.doubleclick.net	United States		15169	GOOGLEUS	false
198.47.127.20	spug-amsfpairbc.pubmnet.com	United States		62713	AS-PUBMATICUS	false
142.250.184.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.180.162	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
64.202.112.95	unknown	United States		22075	AS-OUTBRAINUS	false
13.224.103.39	cdn.p-n.io	United States		16509	AMAZON-02US	false
52.213.98.59	syncelb-831046328.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
23.211.6.95	contextual.media.net	United States		16625	AKAMAI-ASUS	false
142.250.184.98	pagead46.l.doubleclick.net	United States		15169	GOOGLEUS	false
3.127.159.147	unknown	United States		16509	AMAZON-02US	false
141.95.171.142	green.erne.co	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
13.224.103.32	s.ad.smaato.net	United States		16509	AMAZON-02US	false
13.224.100.141	d1ykf07e75w7ss.cloudfront.net	United States		16509	AMAZON-02US	false
13.224.103.30	d2dwiwtjj7ipd3.cloudfront.net	United States		16509	AMAZON-02US	false
3.122.125.162	elb-aws-fr-dorpat-283474803.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
13.224.95.38	cdn.parsely.com	United States		16509	AMAZON-02US	false
54.87.63.104	api.parsely.com	United States		14618	AMAZON-AESUS	false
213.19.147.45	sync.1rx.io	United Kingdom		26120	RHYTHMONEUS	false
185.184.8.90	creativecdn.com	Poland		204995	RTB-HOUSE-AMSNL	false
13.224.98.28	d15kdpgjg3unno.cloudfront.net	United States		16509	AMAZON-02US	false
104.22.24.87	spl.zeotap.com	United States		13335	CLOUDFLARENETUS	false
69.166.1.10	iad-2-sync.go.sonobi.com	United States		27630	AS-XFERNETUS	false
13.224.103.24	sb.scorecardresearch.com	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800684
Start date and time:	2023-02-07 18:06:28 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.familyproof.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@64/0@184/100
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): SgrmBroker.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.4.90, 142.250.184.99, 34.104.35.123, 142.250.184.67, 142.250.180.138, 23.10.249.163, 23.0.174.24, 142.250.184.66, 104.18.33.19, 172.64.154.237, 142.250.180.170, 142.251.209.10, 142.251.209.42, 142.250.184.74, 142.250.184.106, 23.35.236.201, 23.211.4.12, 142.251.209.2, 23.10.249.34, 23.10.249.26, 2.16.13.48, 104.77.32.87, 23.33.72.39, 37.157.5.142, 37.157.5.141, 142.250.184.97, 142.250.180.163, 23.37.42.132, 46.228.164.11, 151.101.2.49, 151.101.66.49, 151.101.130.49, 151.101.194.49, 69.173.144.139, 69.173.144.138, 69.173.144.165, 23.35.237.86, 89.207.16.204, 89.207.16.140, 173.231.180.197, 72.251.241.204, 63.251.232.165, 173.231.181.122, 72.251.245.181, 63.251.232.170, 72.251.241.196, 72.251.241.206, 193.0.160.129, 63.215.202.137, 204.79.197.200, 13.107.21.200, 13.107.42.14, 104.16.88.20, 104.16.89.20, 104.16.87.20, 104.16.85.20, 104.16.86.20, 23.35.236.188
- Excluded domains from analysis (whitelisted): a267.g.akamai.net, secure2.cdn.fastclick.net.edgekey.net, uipglob.trafficmanager.net, partner.googleadservices.com, usersync-geo-global.usersync-prod-sas.akadns.net, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, e9957.b.akamaiedge.net, htlb.casalemedia.com.cdn.cloudflare.net, l-0005.l-msedge.net, e16604.g.akamaiedge.net, update.googleapis.com, www.gstatic.com, rtb-csync-geo.usersync-prod-sas.akadns.net, secure-adnxs.edgekey.net, e9957.e4.akamaiedge.net, fonts.googleapis.com, fs.microsoft.com, e8960.b.akamaiedge.net, content-autofill.googleapis.com, dual-a-0001.a-msedge.net, d5296a202f355bfe85a565c9b5cff9d6.safeframe.googlesyndication.com, a-emea.rfihub.com.akadns.net, pagead2.googlesyndication.com, wildcard.outbrain.com.edgekey.net, edgedl.me.gvt1.com, c.bing.com, rtb.adgrx.com.tech.akadns.net, e6603.g.akamaiedge.net, eus.rubiconproject.com.edgekey.net, e10883.g.akamaiedge.net, um.indexww.com.akadns.net, tpdads.com.edgesuite.net, at.teads.t
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

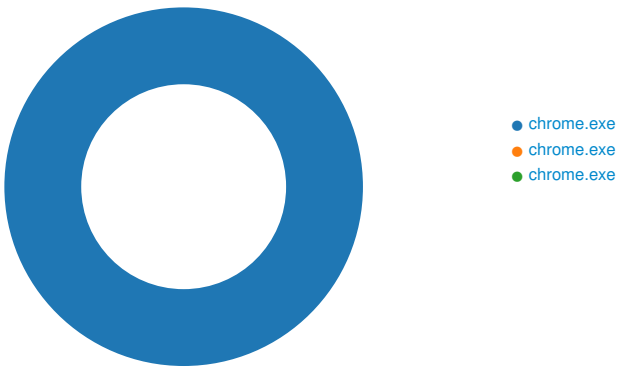
No static file info

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5932, Parent PID: 1836

General

Target ID:	0
Start time:	18:07:33
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: 3460, Parent PID: 5932

General

Target ID:	1
Start time:	18:07:34
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1884 --field-trial-handle=1648,i,15664817480715420111,2584482007518194518,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **4516**, Parent PID: **1836**

General

Target ID:	2
Start time:	18:07:35
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://www.familyproof.com
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly